## Claims

What is claimed is:

1. A method of implementing a data access control facility, said method comprising:

assigning personally identifying information (PII) classification labels to PII data objects, wherein a PII data object has one PII classification label assigned thereto;

defining at least one PII purpose serving function set (PSFS) comprising a list of application functions that read or write PII data objects; and

assigning a PII classification label to each PSFS, wherein a PII data object is only read accessible via an application function of a PII PSFS having a PII classification label that is equal to or a proper subset of the PII classification label of the PII data object.

2. The method of claim 1, wherein a PII data object is write accessible by an application function of a PII PSFS having a PII classification label that is equal to or dominant of the PII classification label of the PII data object.

3. The method of claim 2, wherein the PII data object may be write accessible by an application function of a PII PSFS having a list of PII reclassifications which are allowed to that PII PSFS.

4. The method of claim 1, further comprising identifying a user invoking a particular function of the data access control facility, and assigning a PII clearance set to the identified user, wherein the PII clearance set comprises a list of one or more PII classification labels for the identified user.

5. The method of claim 1, wherein the PII classification label assigned to the PII data object includes an identification of an owner of the PII data object.

6. The method of claim 1, wherein the PII classification label assigned to the PII data object includes an indication of at least one purpose for which the data object may be used.

7. The method of claim 1, further comprising initially defining PII purposes within an enterprise to use the data access control facility, and employing the PII purposes in defining the PII classification labels assigned to the PII data objects and assigned to the at least one PSFS.

8. A data access control method comprising:

(i) invoking, by a user of a data access control facility, a particular function, said data access control facility having personally identifying information (PII) classification labels assigned to PII data objects and at least one PII purpose serving function set (PSFS) including a list of application functions that read, write or reclassify PII data objects, and having a PII classification label assigned thereto, and wherein the user of the data access control facility has assigned thereto a PII clearance set, the PII clearance set for the user comprising a list containing at least one PII classification label;

(ii) determining whether the particular function is defined to a PII PSFS of the at least one PII PSFS of the data access control facility, and if so, determining whether the user's PII clearance set includes a PII classification label matching the PII classification label assigned to that PII PSFS, and if so, allowing access to the particular function; and

(iii) determining whether the user is permitted access to a selected data object to perform the particular function.

9. The data access control method of claim 8, further comprising, prior to said invoking, establishing a process within an operating system under security control of the data access control facility, and wherein said invoking occurs within said established process.

10. The data access control method of claim 9, wherein said determining (ii) further comprises denying access to the particular function if the particular function is not defined to a PII PSFS of the data access control facility, and a current process label (CPL) has been previously set for the established process.

11. The data access control method of claim 9, wherein said determining (iii) comprises determining whether the selected data object comprises a PII data object, and if so, verifying that the user's particular function is defined to a PII PSFS of the at least one PII PSFS of the data access control facility, and if not, denying access to the selected data object.

12. The data access control method of claim 9, wherein said determining (iii) further comprises determining whether a current process label (CPL) has been set for the established process if the selected data object is other than a PII data object, and if not, rendering an access decision to the selected data object via discretionary access control checking.

13. The data access control method of claim 12, wherein said determining (iii) further comprises determining whether the particular function is a read operation if the CPL has been previously set for the process and the selected data object is other than a PII data object, and if so, then rendering an access decision to the selected data object via discretionary access control checking, and if the particular function is other than a read operation, denying access to the selected data object from the established process.

14. The data access control method of claim 11, wherein said determining (iii) further comprises determining whether the particular function comprises a read operation, and if so, determining whether the PII classification label assigned to the PII PSFS to which the particular function is defined is equal to or a proper subset of a PII classification label associated with the selected data object, and if not, denying access to the selected data object, and if so, adding the PII classification label of the selected data object to a current process label (CPL) list for the established process.

15. The data access control method of claim 11, wherein said determining (iii) further comprises determining that the particular function is other than a read operation, and when so, determining whether a current process label (CPL) list for the established process exists, and if not, allowing an access decision to the selected data object to proceed via discretionary access control checking.

16. The data access control method of claim 15, wherein if the CPL list for the established process exists, determining whether the PII classification label of the selected data object is equal to or a proper subset of each of the CPL entries, and if so, allowing an access decision to the selected data object to proceed via discretionary access control checking.

17. The data access control method of claim 16, wherein if the PII classification of the PII data object is not equal to or a proper subset of the PII classification label of each CPL list entry, then the method further comprises determining whether the PII PSFS to which the particular function is defined allows reclassification from the PII classification label(s) in the CPL list to the PII classification label of the PII data object, and if so, allowing an access decision to the selected data object to proceed via discretionary access control checking, otherwise, denying the user access to the PII data object.

18. The data access control method of claim 11, further comprising providing a current process label (CPL) list for the established process, the CPL list comprising a dynamic list of the PII classification labels of each PII data object read within the established process.

19. The data access control method of claim 18, further comprising employing the CPL list when determining whether to allow the user of the established process to access another PII data object when the particular function is a write operation to the another PII data object, wherein the another PII data object may have a different PII classification label than the PII classification label associated with the PII data object from which the information was read, thereby reclassifying the information that was read.

20. The data access control method of claim 19, further comprising providing a "reclassification allowed" parameter associated with the at least one PII PSFS, wherein if the "reclassification allowed" parameter is set, the parameter is associated with all functions defined within the corresponding at least one PII PSFS, and the parameter allows the user executing one of these functions to reclassify a PII data object when writing information into the PII data object that has a PII classification label that is not identical to or a proper subset of each of the PII classification labels contained in the CPL list.

21. A system for implementing a data access control facility, said system comprising:

means for assigning personally identifying information (PII) classification labels to PII data objects, wherein a PII data object has one PII classification label assigned thereto;

means for defining at least one PII purpose serving function set (PSFS) comprising a list of application functions that read or write PII data objects; and

means for assigning a PII classification label to each PSFS, wherein a PII data object is only read accessible via an application function of a PII PSFS having a PII classification label that is equal to or a proper subset of the PII classification label of the PII data object.

22. The system of claim 21, wherein a PII data object is write accessible by an application function of a PII PSFS having a PII classification label that is equal to or dominant of the PII classification label of the PII data object.

23. The system of claim 22, wherein the PII data object may be write accessible by an application function of a PII PSFS having a list of PII reclassifications which are allowed to that PII PSFS.

24. The system of claim 21, further comprising means for identifying a user invoking a particular function of the data access control facility, and for assigning a PII clearance set to the identified user, wherein the PII clearance set comprises a list of one or more PII classification labels for the identified user.

25. The system of claim 21, wherein the PII classification label assigned to the PII data object includes an identification of an owner of the PII data object.

26. The system of claim 21, wherein the PII classification label assigned to the PII data object includes an indication of at least one purpose for which the data object may be used.

27. The system of claim 21, further comprising initially defining PII purposes within an enterprise to use the data access control facility, and employing the PII purposes in defining the PII classification labels assigned to the PII data objects and assigned to the at least one PSFS.

28. A data access control facility comprising:

(i) means for invoking, by a user of a data access control facility, a particular function, said data access control facility having personally identifying information (PII) classification labels assigned to PII data objects and at least one PII purpose serving function set (PSFS) including a list of application functions that read, write or reclassify PII data objects, and having a PII classification label assigned thereto, and wherein the user of the data access control facility has assigned thereto a PII clearance set, the PII clearance set for the user comprising a list containing at least one PII classification label;

(ii) means for determining whether the particular function is defined to a PII PSFS of the at least one PII PSFS of the data access control facility, and if so, determining whether the user's PII clearance set includes a PII classification label matching the PII classification label assigned to that PII PSFS, and if so, allowing access to the particular function; and

(iii) means for determining whether the user is permitted access to a selected data object to perform the particular function.

29. The data access control facility of claim 28, further comprising, prior to said invoking, means for establishing a process within an operating system under security control of the data access control facility, and wherein said invoking occurs within said established process.

30. The data access control facility of claim 29, wherein said means for determining (ii) further comprises means for denying access to the particular function if the particular function is not defined to a PII PSFS of the data access control facility, and a current process label (CPL) has been previously set for the established process.

31. The data access control facility of claim 29, wherein said means for determining (iii) comprises means for determining whether the selected data object comprises a PII data object, and if so, for verifying that the user's particular function is defined to a PII PSFS of the at least one PII PSFS of the data access control facility, and if not, for denying access to the selected data object.

32. The data access control facility of claim 29, wherein said means for determining (iii) further comprises means for determining whether a current process label (CPL) has been set for the established process if the selected data object is other than a PII data object, and if not, for rendering an access decision to the selected data object via discretionary access control checking.

33. The data access control facility of claim 32, wherein said means for determining (iii) further comprises means for determining whether the particular function is a read operation if the CPL has been previously set for the process and the selected data object is other than a PII data object, and if so, then for rendering an access decision to the selected data object via discretionary access control checking, and if the particular function is other than a read operation, for denying access to the selected data object from the established process.

34. The data access control facility of claim 31, wherein said means for determining (iii) further comprises means for determining whether the particular function comprises a read operation, and if so, for determining whether the PII classification label assigned to the PII PSFS to which the particular function is defined is equal to or a proper subset of a PII classification label associated with the selected data object, and if not, for denying access to the selected data object, and if so, for adding the PII classification label of the selected data object to a current process label (CPL) list for the established process.

35. The data access control facility of claim 31, wherein said means for determining (iii) further comprises means for determining that the particular function is other than a read operation, and when so, for determining whether a current process label (CPL) list for the established process exists, and if not, for allowing an access decision to the selected data object to proceed via discretionary access control checking.

36. The data access control facility of claim 35 wherein if the CPL list for the established process exists, means for determining whether the PII classification label of the selected data object is equal to or a proper subset of each of the CPL entries, and if so, for allowing an access decision to the selected data object to proceed via discretionary access control checking.

37. The data access control facility of claim 36, wherein if the PII classification of the PII data object is not equal to or a proper subset of the PII classification label of each CPL list entry, then the facility further comprises means for determining whether the PII PSFS to which the particular function is defined allows reclassification from the PII classification label(s) in the CPL list to the PII classification label of the PII data object, and if so, for allowing an access decision to the selected data object to proceed via discretionary access control checking, otherwise, for denying the user access to the PII data object.

38. The data access control facility of claim 31, further comprising means for providing a current process label (CPL) list for the established process, the CPL list comprising a dynamic list of the PII classification labels of each PII data object read within the established process.

39. The data access control facility of claim 38, further comprising means for employing the CPL list when determining whether to allow the user of the established process to access another PII data object when the particular function is a write operation to the another PII data object, wherein the another PII data object may have a different PII classification label than the PII classification label associated with the PII data object from which the information was read, thereby reclassifying the information that was read.

40. The data access control facility of claim 39, further comprising means for providing a "reclassification allowed" parameter associated with the at least one PII PSFS, wherein if the "reclassification allowed" parameter is set, the parameter is associated with all functions defined within the corresponding at least one PII PSFS, and the parameter allows the user executing one of these functions to reclassify a PII data object when writing information into the PII data object that has a PII classification label that is not identical to or a proper subset of each of the PII classification labels contained in the CPL list.

41. At least one program storage device readable by a machine, embodying at least one program of instructions executable by the machine to perform a method of implementing a data access control facility, said method comprising:

assigning personally identifying information (PII) classification labels to PII data objects, wherein a PII data object has one PII classification label assigned thereto;

defining at least one PII purpose serving function set (PSFS) comprising a list of application functions that read or write PII data objects; and

assigning a PII classification label to each PSFS, wherein a PII data object is only read accessible via an application function of a PII PSFS having a PII classification label that is equal to or a proper subset of the PII classification label of the PII data object.

42. The at least one program storage device of claim 41, wherein a PII data object is write accessible by an application function of a PII PSFS having a PII classification label that is equal to or dominant of the PII classification label of the PII data object.

43. The at least one program storage device of claim 42, wherein the PII data object may be write accessible by an application function of a PII PSFS having a list of PII reclassifications which are allowed to that PII PSFS.

44. The at least one program storage device of claim 41, further comprising identifying a user invoking a particular function of the data access control facility, and assigning a PII clearance set to the identified user, wherein the PII clearance set comprises a list of one or more PII classification labels for the identified user.

45. The at least one program storage device of claim 41, wherein the PII classification label assigned to the PII data object includes an identification of an owner of the PII data object.

46. The at least one program storage device of claim 41, wherein the PII classification label assigned to the PII data object includes an indication of at least one purpose for which the data object may be used.

47. The at least one program storage device of claim 41, further comprising initially defining PII purposes within an enterprise to use the data access control facility, and employing the PII purposes in defining the PII classification labels assigned to the PII data objects and assigned to the at least one PSFS.

48. At least one program storage device readable by a machine, embodying at least one program of instructions executable by the machine to perform a method for controlling data access, said method comprising:

(i) invoking, by a user of a data access control facility, a particular function, said data access control facility having personally identifying information (PII) classification labels assigned to PII data objects and at least one PII purpose serving function set (PSFS) including a list of application functions that read, write or reclassify PII data objects, and having a PII classification label assigned thereto, and wherein the user of the data access control facility has assigned thereto a PII clearance set, the PII clearance set for the user comprising a list containing at least one PII classification label;

(ii) determining whether the particular function is defined to a PII PSFS of the at least one PII PSFS of the data access control facility, and if so, determining whether the user's PII clearance set includes a PII classification label matching the PII classification label assigned to that PII PSFS, and if so, allowing access to the particular function; and

(iii) determining whether the user is permitted access to a selected data object to perform the particular function.

49. The at least one program storage device of claim 48, further comprising, prior to said invoking, establishing a process within an operating system under security control of the data access control facility, and wherein said invoking occurs within said established process.

50. The at least one program storage device of claim 49, wherein said determining (ii) further comprises denying access to the particular function if the particular function is not defined to a PII PSFS of the data access control facility, and a current process label (CPL) has been previously set for the established process.

51. The at least one program storage device of claim 49, wherein said determining (iii) comprises determining whether the selected data object comprises a PII data object, and if so, verifying that the user's particular function is defined to a PII PSFS of the at least one PII PSFS of the data access control facility, and if not, denying access to the selected data object.

52. The at least one program storage device of claim 49, wherein said determining (iii) further comprises determining whether a current process label (CPL) has been set for the established process if the selected data object is other than a PII data object, and if not, rendering an access decision to the selected data object via discretionary access control checking.

53. The at least one program storage device of claim 52, wherein said determining (iii) further comprises determining whether the particular function is a read operation if the CPL has been previously set for the process and the selected data object is other than a PII data object, and if so, then rendering an access decision to the selected data object via discretionary access control checking, and if the particular function is other than a read operation, denying access to the selected data object from the established process.

54. The at least one program storage device of claim 51, wherein said determining (iii) further comprises determining whether the particular function comprises a read operation, and if so, determining whether the PII classification label assigned to the PII PSFS to which the particular function is defined is equal to or a proper subset of a PII classification label associated with the selected data object, and if not, denying access to the selected data object, and if so, adding the PII classification label of the selected data object to a current process label (CPL) list for the established process.

55. The at least one program storage device of claim 51, wherein said determining (iii) further comprises determining that the particular function is other than a read operation, and when so, determining whether a current process label (CPL) list for the established process exists, and if not, allowing an access decision to the selected data object to proceed via discretionary access control checking.

56. The at least one program storage device of claim 55, wherein if the CPL list for the established process exists, determining whether the PII classification label of the selected data object is equal to or a proper subset of each of the CPL entries, and if so, allowing an access decision to the selected data object to proceed via discretionary access control checking.

57. The at least one program storage device of claim 56, wherein if the PII classification of the PII data object is not equal to or a proper subset of the PII classification label of each CPL list entry, then the method further comprises determining whether the PII PSFS to which the particular function is defined allows reclassification from the PII classification label(s) in the CPL list to the PII classification label of the PII data object, and if so, allowing an access decision to the selected data object to proceed via discretionary access control checking, otherwise, denying the user access to the PII data object.

58. The at least one program storage device of claim 51, further comprising providing a current process label (CPL) list for the established process, the CPL list comprising a dynamic list of the PII classification labels of each PII data object read within the established process.

59. The at least one program storage device of claim 58, further comprising employing the CPL list when determining whether to allow the user of the established process to access another PII data object when the particular function is a write operation to the another PII data object, wherein the another PII data object may have a different PII classification label than the PII classification label associated with the PII data object from which the information was read, thereby reclassifying the information that was read.

60. The at least one program storage device of claim 59, further comprising providing a "reclassification allowed" parameter associated with the at least one PII PSFS, wherein if the "reclassification allowed" parameter is set, the parameter is associated with all functions defined within the corresponding at least one PII PSFS, and the parameter allows the user executing one of these functions to reclassify a PII data object when writing information into the PII data object that has a PII classification label that is not identical to or a proper subset of each of the PII classification labels contained in the CPL list.

* * * * *